

IN THE UNITED STATES DISTRICT COURT  
FOR THE NORTHERN DISTRICT OF TEXAS  
DALLAS DIVISION

---

UNITED STATES OF AMERICA

v.

ANDREW KASNETZ

No. 3:18-CR-345-O  
**ECF**

**GOVERNMENT’S NOTICE OF EXPERT TESTIMONY**

The United States of America (“the government”), files this, the Government’s Notice of Expert Testimony, in the above-captioned case.

1. Aaron Covey  
Federal Bureau of Investigation (“FBI”)  
Dallas, Texas

Covey is an agent with the FBI. Covey’s testimony will be based on his knowledge, skills, training, and experience in the area of computer forensics, computer forensic tools and analysis, the Internet, and his forensic review and analysis of the relevant electronic devices—particularly a HP desktop computer and Samsung laptop computer (Devices)---seized from Kasnetz pursuant to a search warrant.

Covey is expected to testify about his review of the Devices seized from, and used by, Kasnetz to access and view child pornography. These Devices have been made available—and continue to remain available—for examination by the defense.

Specifically, Covey is expected to testify that the forensic evidence on the Devices used by Kasnetz is consistent with the allegations that Kasnetz accessed with intent to view

child pornography, receive and possessed it (see e.g. Counts One and Two of the indictment). Covey is also expected to testify that the forensic evidence on the HP desktop computer used by Kasnetz revealed the same child pornography images that Kasnetz is charged with in Counts One and Two of the indictment or any superseding indictment. Some of the forensic steps and artifacts regarding the Devices have been memorialized in reports, and Covey will explain the significance of those findings. In addition, Covey reviewed the Devices with forensic tools and will opine to his findings based on those forensic tools.

Covey may also testify regarding the following subject matters:

- Regarding the Internet, internet service providers, IP addresses, including the interstate nature of the Internet and how use of the Internet affects the forensic evidence within an electronic device;
- Regarding how computers receive information and data through the Internet, and how files are transferred to, and stored within, electronic devices, including thumbcache images, data in unallocated space, and hashes;
- Regarding forensic evidence suggesting that someone has tried to delete material from an electronic device;
- Regarding forensic tools commonly accepted and used to examine the user activity and content of an electronic device, including but not limited to Internet Evidence Finder, FTK Imager, and other tools and results of such tools that have been run on the laptop computer Kasnetz used;
- Regarding evidence of web browsing, including but not limited to, file paths, cookie files, internet history, bookmarks, and other Internet-based communications stored in electronic devices, including in temporary Internet file folders, file slack, and unallocated space.

Defense counsel has been provided with a copy this witness's reports of

examination and his professional qualifications.

2. Rob Erdley  
Pennsylvania State Police (retired)  
Indiana, PA

Erdley may testify regarding the following subject matters:

- Regarding the Internet, internet service providers, IP addresses, including the interstate nature of the Internet and how use of the Internet affects the forensic evidence within an electronic device;
- Regarding how computers receive information and data through the Internet, and how files are transferred to, and stored within, electronic devices, including thumbcache images, data in unallocated space, and hashes;
- Regarding forensic evidence suggesting that someone has tried to delete material from an electronic device;
- Regarding forensic tools commonly accepted and used to examine the user activity and content of an electronic device, including but not limited to Internet Evidence Finder, FTK Imager, and other tools and results of such tools that have been run on the laptop computer Kasnetz used;
- Regarding evidence of web browsing, including but not limited to, file paths, cookie files, internet history, bookmarks, and other Internet-based communications stored in electronic devices, including in temporary Internet file folders, file slack, and unallocated space.
- How the BitTorrent file sharing network works. How BitTorrent investigative software works. His review of the evidence in this case and the meaning of the entries in the logs. He is expected to refute claims made by defendant's expert that there are errors that undermine claims made in the charges against defendant or other claims made by that expert.

3. Jeff Rich  
Plano Police Department  
Plano, TX

Jeff Rich is a detective with the Plano Police Department. Jeff Rich will testify

that from October to November 2017, he downloaded child sexual abuse material from an IP address that was ultimately connected to Kasnetz's home.

Rich may also testify regarding the following subject matters:

- Regarding the Internet, internet service providers, IP addresses, including the interstate nature of the Internet and how use of the Internet affects the forensic evidence within an electronic device;
- Regarding how computers receive information and data through the Internet, and how files are transferred to, and stored within, electronic devices, including thumbcache images, data in unallocated space, and hashes;
- Regarding forensic evidence suggesting that someone has tried to delete material from an electronic device;
- Regarding forensic tools commonly accepted and used to examine the user activity and content of an electronic device, including but not limited to Internet Evidence Finder, FTK Imager, and other tools and results of such tools that have been run on the laptop computer Kasnetz used;
- Regarding evidence of web browsing, including but not limited to, file paths, cookie files, internet history, bookmarks, and other Internet-based communications stored in electronic devices, including in temporary Internet file folders, file slack, and unallocated space.
- How the BitTorrent file sharing network works. How BitTorrent investigative software works. His review of the evidence in this case and the meaning of the entries in the logs. He is expected to refute claims made by defendant's expert that there are errors that undermine claims made in the charges against defendant or others claims made by that expert.

4. Eric Weast  
Dallas Police Department  
Dallas, TX

Eric Weast is a detective with the Dallas Police Department. On February 20,

2018, he assisted with the execution of a search warrant at Kasnetz's home. Weast's testimony will be based on his knowledge, skills, training, and experience in the area of computer forensics, computer forensic tools and analysis, the Internet, and his forensic review and analysis of the relevant electronic devices—a HP desktop computer and Samsung laptop computer (Devices) seized from Kasnetz pursuant to a search warrant.

Weast is expected to testify about his review of the Devices seized from, and used by, Kasnetz to access and view child pornography. These Devices have been made available—and continue to remain available—for examination by the defense.

Specifically, Weast is expected to testify that the forensic evidence on the Devices used by Kasnetz is consistent with the allegations that Kasnetz accessed with intent to view child pornography, receive and possessed it (see e.g. Counts One and Two of the indictment or the superseding indictment). Weast is also expected to testify that the forensic evidence on the HP desktop computer used by Kasnetz revealed the same child pornography images that Kasnetz is charged with in Counts One and Two of the indictment. Some of the forensic steps and artifacts regarding the Devices have been memorialized in reports, and Weast will explain the significance of those findings. In addition, Weast reviewed the Devices with forensic tools and will opine to his findings based on those forensic tools.

Weast may also testify regarding the following subject matters:

- Regarding the Internet, internet service providers, IP addresses, including the interstate nature of the Internet and how use of the Internet affects the forensic evidence within an electronic device;

- Regarding how computers receive information and data through the Internet, and how files are transferred to, and stored within, electronic devices, including thumbcache images, data in unallocated space, and hashes;
- Regarding forensic evidence suggesting that someone has tried to delete material from an electronic device;
- Regarding forensic tools commonly accepted and used to examine the user activity and content of an electronic device, including but not limited to Internet Evidence Finder, FTK Imager, and other tools and results of such tools that have been run on the laptop computer Kasnetz used;
- Regarding evidence of web browsing, including but not limited to, file paths, cookie files, internet history, bookmarks, and other Internet-based communications stored in electronic devices, including in temporary Internet file folders, file slack, and unallocated space.

Defense counsel has been provided with a copy this witness's reports of examination and his professional qualifications.

Respectfully submitted,

ERIN NEALY COX  
UNITED STATES ATTORNEY

*s/ Shane Read*

SHANE READ  
Assistant United States Attorney  
Texas State Bar No. 16623950  
1100 Commerce Street, 3rd Floor  
Dallas, Texas 75242  
Telephone: 214.659.8600  
Email: shane.read@usdoj.gov

**CERTIFICATE OF SERVICE**

I hereby certify that on **September 16, 2020**, I electronically filed the foregoing document with the Clerk of Court for the United States District Court, Northern District of Texas, using the electronic case filing system of the Court. The electronic case filing system sent a “Notice of Electronic Filing” to attorney(s) of record who have consented in writing to accept this Notice as service of this document by electronic means.

*s/ Shane Read*

SHANE READ  
Assistant United States Attorney